42390P13769   PATENT

REMARKS

Claims 2-4 and 6-13 are pending in the application. Claim 3 is independent. Claims 1, 5 and 14-34 have been canceled.

Claims 2-4 and 6-13 have been rejected under 35 U.S.C. §102(e), as being anticipated by U.S. Patent No. 6,651,171 ("England").

In response, it is argued that independent claim 3 includes at least one limitation not disclosed by England.

First, independent claim 3 includes a limitation of receiving, by a processor, an instruction to launch a code module to establish a trusted system environment. The examiner argues that England discloses this limitation in lines 42-44 of column 8, which describes an instruction decoder. England does not describe a trusted system environment, a code module to establish a trusted system environment, or an instruction to launch a code module to establish a trusted system environment.

Second, independent claim 3 includes a limitation of verifying, by the processor in response to receiving the instruction, that the environment of the processor is appropriate to launch the code module. The examiner argues that England discloses this limitation in lines 53-54 of column 8, lines 60-65 of column 9, and lines 40-44 of column 15, which describe a specification of memory addresses to be curtained, determining whether or not to execute curtained code, and a processor with system management mode. None of these are the same as verifying the environment of a processor in response to receiving an instruction, or verifying that the environment of a processor is appropriate to launch of code module, and England does not describe this limitation elsewhere.

Third, independent claim 3 includes a limitation of updating, by the processor in response to verifying that the environment of the processor is appropriate, event processing to support launching the code module. The examiner argues that England discloses this limitation in lines 34-48 of column 8, which describes the control unit of a processor. England does not describe updating event processing to support launching the code module.

2

42390P13769   PATENT

Fourth, independent claim 3 includes a limitation of configuring, by the processor in response to locking the processor bus, a cache memory of a processor to operate in a private mode in which requests within the memory range of the cache are satisfied by the cache and cache lines are not replaced or invalidated in response to snoop requests on the processor bus. Fifth, independent claim 3 includes a limitation of transferring, by the processor in response to configuring the cache memory to operate in the private mode, the code module to the cache memory. Sixth, independent claim 3 includes a limitation of determining, by the processor in response to transferring the code module to the cache memory, that the code module stored in the cache memory is authentic. Seventh, independent claim 3 includes a limitation of executing the code module from the cache memory in response to determining that the code module is authentic. England does not describe any of these limitations. It is not clear, based on the examiner's citations or otherwise, what in England that the examiner believes corresponds to the cache memory or the code module of claim 3 of the present invention.

Each of dependent claims 2, 4, and 6-13 include at least one limitation not disclosed by England based at least on their dependence on independent claim 3, as amended. Accordingly, the withdrawal of the rejections of claims 2-4 and 6-13 under 35 U.S.C. §102(e) is respectfully requested.
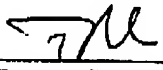
3

42390P13769

AUG 1 8 2008   PATENT

CONCLUSION

Based on the foregoing, it is respectfully submitted that the rejections of claims 2-4 and 6-13 have been overcome, and that these claims are in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Please charge any necessary fees, including extension fees, to our Deposit Account No. 50-0221.

Respectfully submitted,

Date: <u>August 18, 2008</u>

Thomas R. Lane
Registration No. 42,781

4